Optimized Mobile Biometric Data Networking

A Project Report
Submitted to the Faculty
of the
UNITED STATES COAST GUARD ACADEMY
in partial fulfillment of the requirements for the
Degree of Bachelor of Science
in
Electrical Engineering
by

*Signature #1*_____
Name 1/c Al Sowers

*Signature #2*_____
Name 1/c Donatas Siaudinis

Projects in Electrical and Computer Engineering

25 April 2008

Reviewed By:

_____
LCDR Daniel K. Pickles, Project Advisor

_____
LCDR Daniel K. Pickles, Class Coordinator

_____
Professor Keith C. Gross, Chief, Electrical & Computer Engineering Section

Abstract

One of the main missions of the United States Coast Guard is the policing of illegal immigration. Since November 2006, the USCG has been exercising the Biometrics at Sea Proof-of-Concept, which utilizes the ability to transfer biometric data taken from migrants attempting to illegally enter the United States via the maritime vector. Biometrics is the measure of physical characteristics of humans based upon one or more intrinsic physical or behavioral traits. Transferring biometric data from deployed Coast Guard cutters with limited bandwidth has proven to be extremely time-intensive; due to the high costs of satellite usage, transferring biometric data in the method currently in practice has been very expensive and has resulted in a substantial unplanned cost for the Coast Guard. The main purpose of the Biometrics at Sea is to check for the previous records of migrants or to see if there are any dangerous or wanted migrants on the Coast Guard platforms. While Biometrics at Sea has been successful, there is much room for improvement. By optimizing the transfer of the biometric data, this proof-of-concept will be able to effectively reduce the cost of Biometrics at Sea by decreasing satellite air time and increasing the availability, reliability, and speed of biometric data transfer.

Introduction

The Optimized Mobile Biometric Data Networking (OMBDN) project is the system senior design project effort to explore the interfaces & uses of the MLCA (Maintenance and Logistics Command Atlantic) Large File Transfer concept with TISCOM Fleet 55 SATCOM and cellular capabilities to optimize biometric transfer methods from underway Coast Guard cutters. This project entails the research of mobile data networking, wireless security, and information assurance to ensure better performance and lower costs for the Coast Guard Biometric at Sea capability. The main purpose of this project is to reduce the recurring operating cost by decreasing satellite air time and to increase the availability, reliability, and speed of biometric data transfer by optimizing the system (Appendix A).

The OMBDN project is co-sponsored by the U.S. Coast Guard Telecommunications & Information Systems Command (TISCOM) Radio Systems division (TSD-3c) in Alexandria, VA, Research and Development (R&D CEN) in Groton, CT, and Maintenance & Logistics Command, Atlantic, in Norfolk, VA. TISCOM is interested in the most efficient transport of the biometric data from the USCG cutters to the United States Visitor and Immigrant Status Indicator Technology (US-VISIT). R&D CEN is interested in the most reliable and repeatable process to scan the biometric data against the US VISIT database. The role of the MLCA is to leverage its proven Large File Transfer concept towards the USCG operational requirements and mission needs (Appendix B).

This paper describes the background information of the Biometrics at Sea effort, defines the overall objectives, and identifies the proposed design solution to optimize the mobile biometric data networking system.

Background

Illegal immigration is one of the most serious problems in the USCG law enforcement and a very hot topic of debate for in the political sphere involved in Homeland Security. For many years foreigners have been trying to enter the US illegally. The USCG implemented the Biometrics at Sea Proof-of-Concept in Puerto Rico in November 2006 to provide a means for boarding teams to identify individuals in real time by means of collecting fingerprint images and checking these images against a government-owned database. In order to expand data collection, the proof-of-concept was expanded to Southern Florida in March 2008. The proof-of-concept entails the collection & transmission of biometric data in order to positively identify migrants attempting to enter the United States illegally via the maritime vector. Biometrics is the measure of physical characteristics of humans based upon one or more intrinsic physical or behavioral traits.

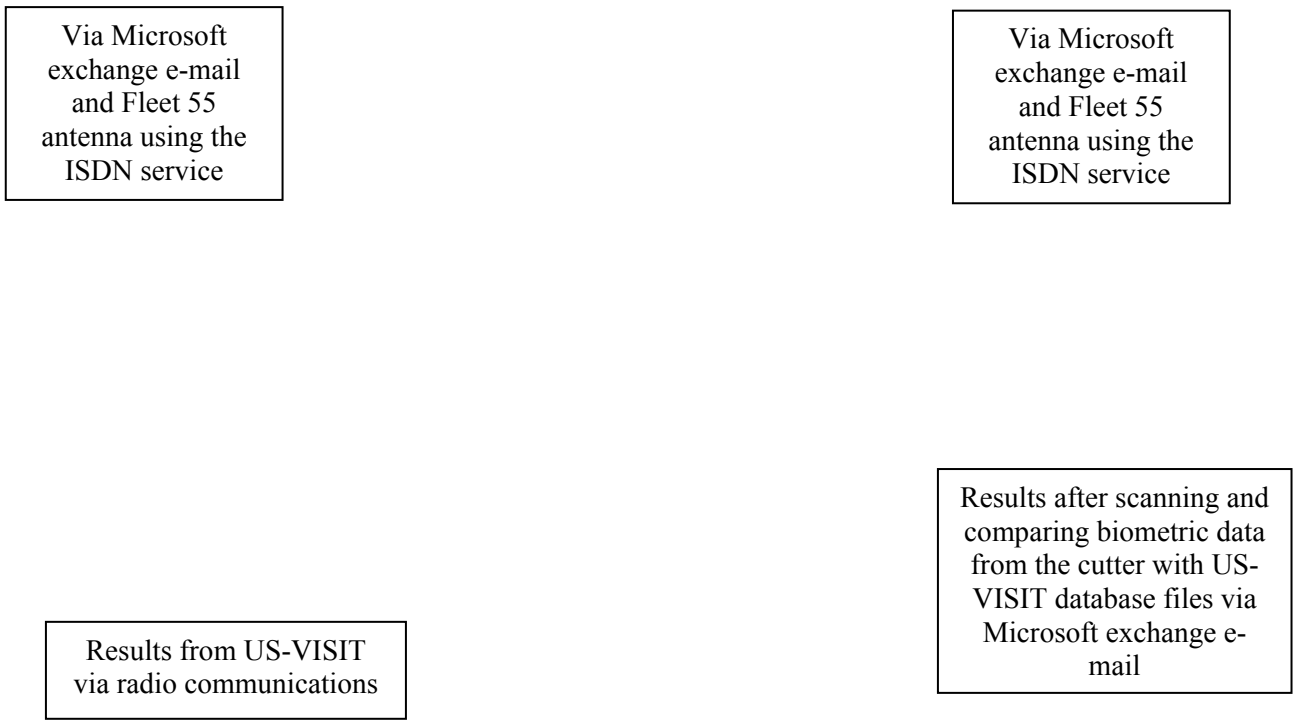


Figure 1. Current biometric file transfer method

Currently, the process by which the Coast Guard collects biometric data includes capturing the digital image of both index fingers as well as the facial image of the migrant. This data is wrapped into a biometric file, roughly 100 kB in size [1]. As seen in Figure 1, the data is transferred to the USCG shore units via the Microsoft Exchange Server. The information for one person is simply being attached to an email and sent to the shore through a Microsoft Exchange Server on the ship. The main data link between a ship and a shore unit is a satellite connection, which must stay on the entire time during the transfer of the data to the US-VISIT database, called IDENT. US-VISIT is an immigration and border management organization. Their database, IDENT, stores the fingerprint images of all foreigners who enter the United States for verification purposes. When foreigners apply for a visa to enter the United States, U.S. Embassies and Consulates around the world submit the applicant's fingerprints to IDENT to verify that the person is who they say they are. In order to ensure that we are not allowing persons with previous criminal records into the country, IDENT includes portions of other law enforcement databases, such as subsets (Watchlist, Known & Suspect Terrorist) of the Federal Bureau of Investigation's database (IAFIS). IDENT uses an algorithm to match minutiae of fingerprints in a one-to-one matching technique. Because of the "one in, one out" method that is inherent to checking identities when individuals are applying for entry into the country, the IDENT database was set up to only accept one fingerprint record at a time (this resulted in the USCG only being able to submit one fingerprint at a time as well). Should the individual have a pre-existing record on IDENT, a response is returned to the visa application office with the history of that individual. It is important to note that, if an individual has an IDENT record, this could only mean that they have entered the United States in the past (whether legally or

illegally). Essentially, US-VISIT's purpose is to keep out the people who could cause harm in the U.S. should we allow them to enter the country legally. The US-VISIT database automatically scans through approximately 100-million records to compare the received data to its archives. In terms of the USCG proof-of-concept, the results of the data analysis are automatically sent to the appropriate Coast Guard Command Center and then transmitted by a radio back to the ship. Responses are communicated from US-VISIT as a "HIT" or "NO HIT"; a "HIT" indicating a record with prior US law violation and "NO HIT" indicating that the individual has never been entered into the database. Individuals not previously entered into the database are subsequently enrolled as a result [2].

The main disadvantages of the current method are the slow speed of service, reliability, repeatability, and high recurring cost. For example, every biometric file received by US-VISIT must be sent in an individual email as an attachment with specific eXtensible Markup Language (XML) formatting because US-VISIT is automated (and because the system was set up for a "one in, one out" method, as previously discussed). Therefore, if a USCG cutter interdicts 100 migrants it would take 100 emails to transfer all the information. The satellite would have to be maintained "on air" and billed per minute until all 100 emails reached their destination at US-VISIT and then confirmed by the Command Center. To send 100 individual emails, each having on average a 100 kb attachment, takes approximately 30-45 minutes, and costs the USCG around $180-$270 [3].

Satellite air time is very expensive. Currently, the Coast Guard is spending $2.85 per Mb for satellite "pay by the bit" service, or $5.60 per minute for satellite "dial on demand" service. The 'by the minute' service is typically used for large file transfers. One disadvantage to the Integrated Service Digital Network (ISDN) satellite service is that it currently transfers at a 50

kbps throughput. However, with the pitch and roll of a patrol boat, the satellite connection is often disrupted and files have to be sent multiple times. Also, the satellite must remain on until the patrol boat receives confirmation from the command center that all the files have been processed by US-VISIT. Patrol boats in Puerto Rico have exceeded 2 hours to complete the transfer the biometric data of 100 migrants. The cost for this connection method can quickly add up. On average, each cutter operating from Puerto Rico is spending approximately $20,833 per month on Internet connectivity. By optimizing the biometric mobile data networking, the Coast Guard could increase its proof-of-concept speed of service, save thousands of dollars per month per cutter, and implement a better information accountability system [3].

Currently, the U.S. Coast Guard Maintenance and Logistics Command Atlantic (MLCA) Large File Transfer concept can be one of the solutions to solve this problem The MLCA has several servers, one of which is capable of storing biometric files that are sent from the cutters. The cutters could send one large file to the MLCA instead of individually sending the biometric files to US-VISIT in an email, one at a time. The MLCA has developed a system that can compress a large size file into a "zip" folder, reducing the size of the file. Using this web application the cutter would be able to shrink the size of the files it is sending, send all biometrics as one bulk zipped file, and decrease the amount of satellite airtime for the cutter [4]. In addition, the *Venturi Wireless* Performance Enhancement Proxy (PEP) server has ability to optimize Transmission Control Protocol (TCP) in the wireless environment. "Venturi Transport Protocol (VTP) is a cross-layer technology that integrates transport layer optimization ─ in the form of the Venturi Transport Protocol (VTP) ─ with Smart Compression technology to provide unmatched improvements in connection speeds, application consistency, coverage availability and network efficiency" [5].

Objective

The main goal of the OMBDN project is to optimize the file transfer of the biometric files from the cutters to US-VISIT. The process includes less satellite air time, a decrease in monthly cost for cutter connectivity, and faster speed of service. To decrease satellite air time, and subsequently decrease the monthly cost of cutter connectivity, the biometric files need to be transferred in a different manner.

Thoroughly outlined in the Functional Requirements Document is several requirements and constraints that must be addressed (Appendix C). Based on file size calculations in conjunction with the transfer rate of the cutters, each biometric data file must be dispatched in 20 seconds or less. If each file reaches its destination in 20 seconds or less, then the overall satellite air time from each cutter will be significantly decreased. The new transfer method system is required to have great reliability so that the mean time between failures is no less than 10,000 hours. Although not turned on 24 hours a day, satellite connectivity must be available to the cutter 95% of the time while they are underway. Also, Coast Guard patrol boats must have Internet connectivity within 200 NM from all United States and territorial coastlines. Lastly, cutters shall not be required to perform technical preventative maintenance or extensive troubleshooting on the solution chosen to optimize the system [6].

Since the mobile biometric file data networking system has already been implemented on the 110' cutter in Puerto Rico, there are a few constraints that must be dealt with when attempting to optimize the transfer of the biometric data. First, each cutter must connect to the Internet through the Fleet 55 via satellite connectivity, Mobile Packet Data Service (MPDS) ("pay by the bit"), ISDN ("pay by the minute"), or cellular services. These are the only three methods through which a Coast Guard Cutter can obtain internet connectivity. Since it has the

faster throughput than MPDS, ISDN is used for large file transfers for cutters that are out of cellular connectivity range. Also, because their system is automated, every email sent to US-VISIT must be in a particular XML format so it can be processed properly.

System Design

The design solution proposed integrates the Coast Guard's MLCA Large File Transfer concept into the current biometric file transfer process presented in Figure 1. The result of the proposed solution, which meets the sponsors needs detailed in the Business Case (Appendix A), is a reduction in satellite air time, a decrease in monthly costs for cutter connectivity, and faster speed of service. To lower satellite air time and subsequently to decrease the monthly cost of cutter connectivity, the biometric files need to be transferred in a different manner (Appendix D) (Figure 2).

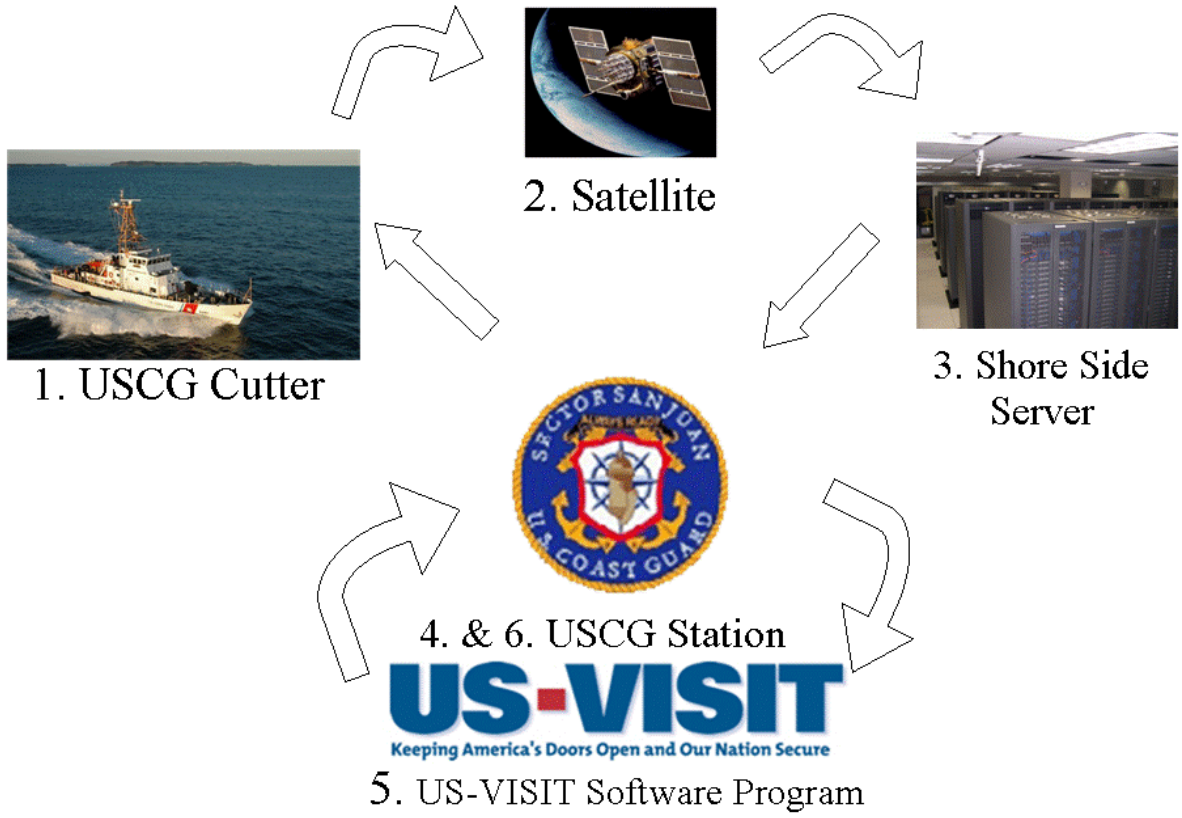


Figure 2: Optimized biometrics file transfer design

The first step in lowering the satellite air time is to get the files from the ship to the shoreside servers as fast as possible. Since the biometric files are to be compressed into one zip file, using WinZip, they may be encrypted with a password protection for transmission. Then, using the MLCA Large File transfer system, cutters would be able to send these large zip files to the MLCA server; a Dell Poweredge 2950 located in Norfolk, VA [7]. The server currently runs Windows 2003 Server Standard R2, and the front end of the server will be designed so that when it receives an email from the cutters, it will automatically generate a response to inform the Coast Guard Command Center that there are biometric files on the server for them to retrieve. The Command Center can log in and access the files by entering the pre-arranged password that was used to encrypt the file.

Sending one large file will decrease satellite air time. The new design of the system shown in Figure 2 will include a transfer status confirmation. This feature will allow the user to be able to visual see when the file has been transferred. Therefore, when the transfer is complete, the cutter can turn off the Fleet 55 and significantly reduce the amount of satellite air time. This optimization will lower the monthly cost of underway connectivity.

Last step in the process is e-mailing the biometric file attachments to US-VISIT. By moving the e-mailing function from the shipboard environment to the Command Center, the process benefits from speed of service, reliability, and reduced recurring operating cost. Command Center is a shore unit where the detailed e-mailing conditions are more constant rather than the dynamic environment at sea. Also, by transferring the biometric data as one compressed file to the shore as fast as possible, the Command Center can send out the individual emails to

the US-VISIT database using a land line, also increasing speed of service since land lines have a much faster and much more reliable connection speed than the 64 kbps of the cutters. The Command Center can get direct replies from US-VISIT and communicate all results back to the ship via radio. Thus, the new method will not only effectively optimize the biometric mobile data networking system and save the Coast Guard time and money, but also will place the duties of sending the files to US-VISIT on the Command Center and allow the CGC Crew's to be active and engaged with the migrants [8].

While developing the Support Plan (Appendix E), some serious ethical and political considerations were identified for this project. Because of the records involved with the biometric data of humans, maintaining privacy and security are very important. Ethically, the Coast Guard is responsible for the protection in not allowing information on migrants to be released to the public. Politically, this biometric data not only helps "police" immigration but also detects multiple offenders and dangerous or at large criminals. By moving from the e-mail based design to the file server design, the security and privacy will improve by eliminating the risk leaving compromising data on Coast Guard e-mail servers.

In a major tenet of the Federal Information Security Management Act of 2002, the CG is required to identify and to provide security of information maintained by the federal agencies against unauthorized access, use, disclosure, disruption, and destruction. The optimized design will employ efficient, information-based security procedures on all information technology. It will also apply an appropriate certification and accreditation (C&A) process to every information system developed by the program sponsor.

Before being transferred from the CG Cutter to the shore side file server, each biometric zip file will be encrypted using a WinZip password which will be known only by the cutter and

the Command Center. Therefore, the data will be secure at all times not only during the transfer but also while on the file server. Only the Command Center Watch Officer with the correct password will be able to pull the files off the file server. Then the biometric files will be automatically deleted after 48 hours to prevent any biometric data being left on the server.

The shore side server consists of ColdFusion application software. "Allaire ColdFusion is a popular web applications development tool. ColdFusion uses a tag-based, server scripting language that is ideal for programming Web applications. Processed entirely on the server, the ColdFusion Markup Language (CFML) cleanly integrates with HTML for user interface and XML for data exchange. Both open and extendible, CFML supports more than 70 server-side tags, 200 functions, and 800 third-party components making it the most productive language available for creating advanced Web applications. In addition, ColdFusion supports Java and C++, and fully integrates with object transaction middleware through COM, CORBA, or EJB" [9].

Results

The Biometrics Mock-Up system that is used in lab for testing consists of two laptop computers and one desktop computer. The first Laptop computer is the Patrol Boat Mock-Up. The second laptop is the File Server Mock-Up. Lastly, the desktop computer is the Command Center Mock-Up. In accordance with the Test Plan (Appendix F), several tests were executed on the mock biometric set up in lab. The test plan diagram is presented in Figure 3.

TEST PLAN DIAGRAM

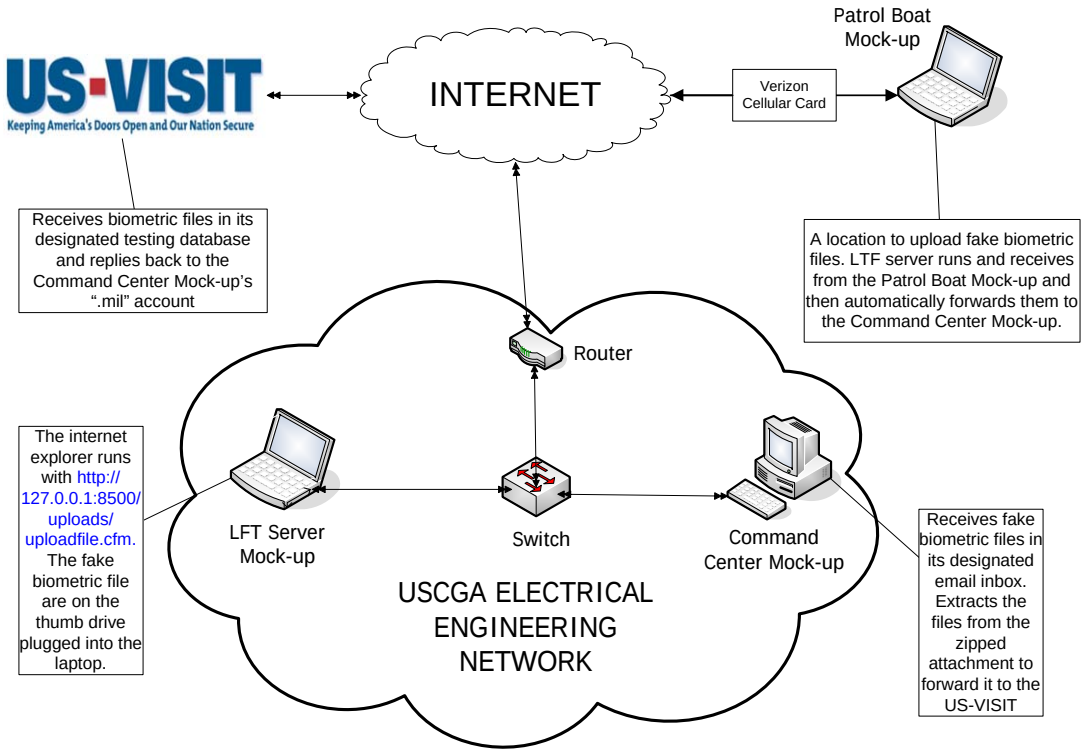
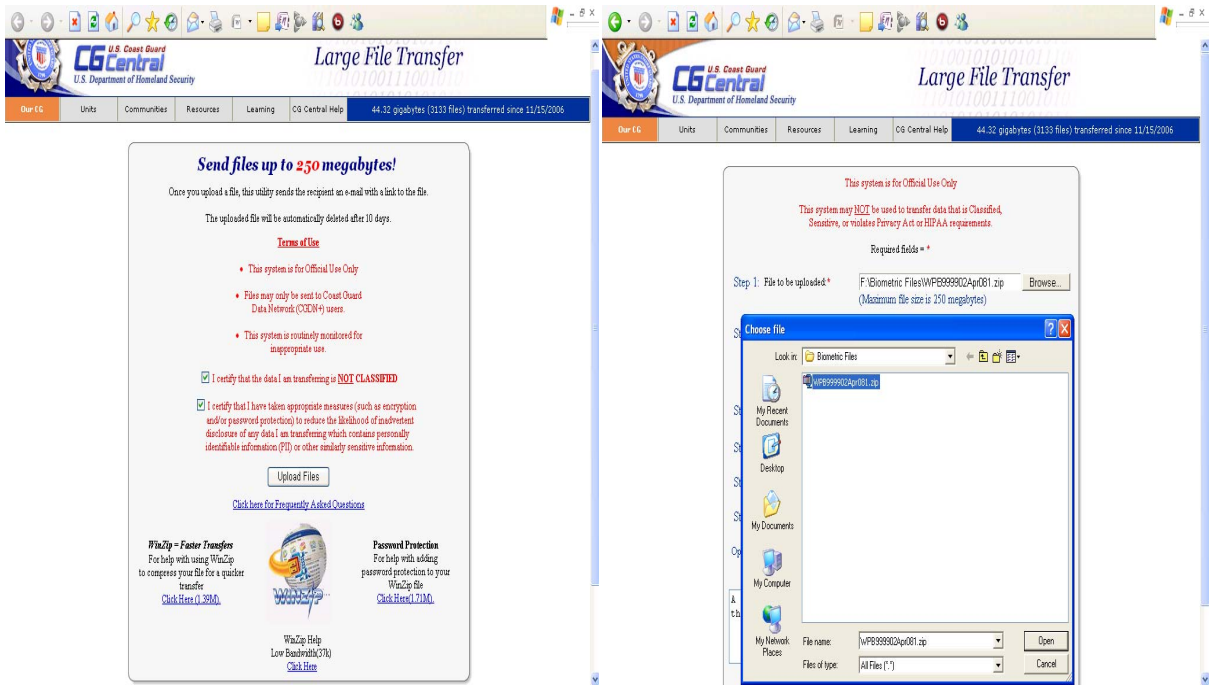


Figure 3. Mock-up System Design

To test the prototype system design 4 tests were conducted. The first test that was conducted was the ability to send zip files containing test biometric files from the patrol boat mock-up to the shore side file server using the large file transfer web application pictured below. Using the LFT web site through the ColdFusion server, the biometric files were uploaded to the server from the Patrol Boat Mock-Up. Below are the LFT web page and a screenshot of how the biometric files were attached.



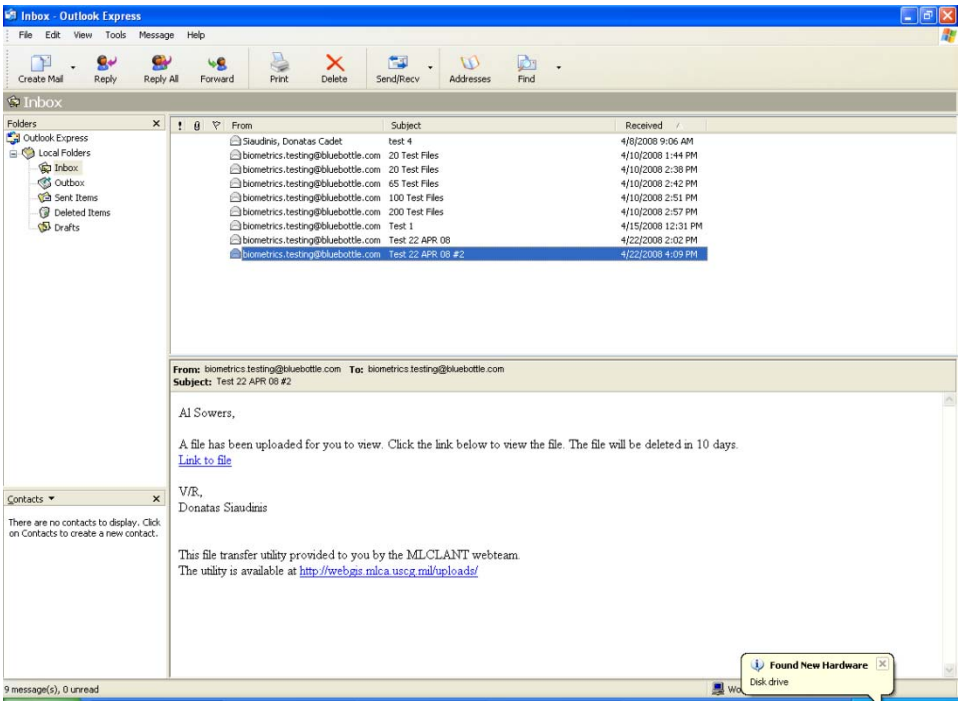
Also, the ability of the file server to send a notification email to the Command Center was tested as well. During this test, 20, 65, 100, 200 test files were sent from the patrol boat mock-up were sent to the file server using the cellular card which provides wireless connectivity to the Internet. The cellular card is used to simulate the cutters wireless connectivity. A stop watch was used to time how long it would take for the files to go from the patrol boat mock-up to the file server and also, how long it takes for the Command Center mock-up to receive the notification email from the file server. The chart below shows the results from the test:

Table 1. Test results

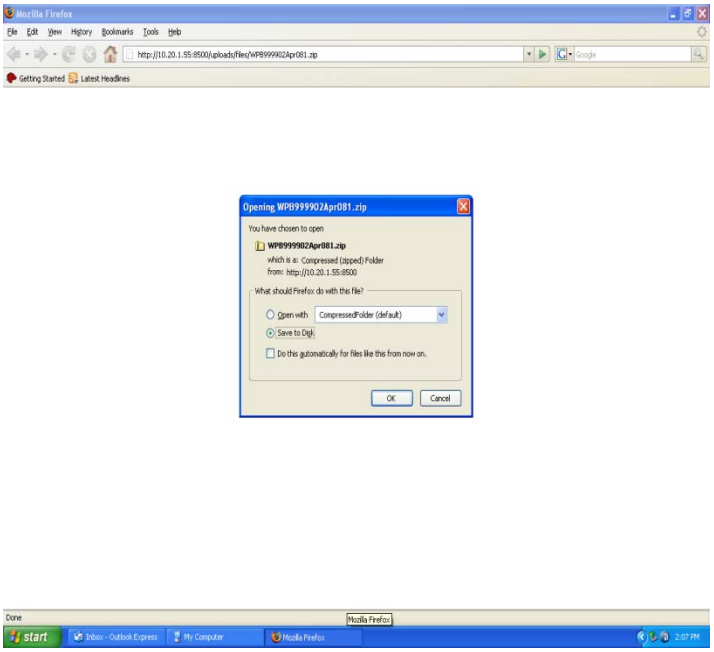
Number of files	Size, kB	Zipping time before transfer, SEC	Cutter-file server transfer time, MIN:SEC	File server-CC notification time, MIN:SEC	Cutter-CC notification time, MIN:SEC
20	1,072	6	0:35	1:37	2:12
65	4,599	6	1:25	1:25	2:52
100	5,412	6	1:47	1:56	3:43
200	10,823	6	4:17	1:37	5:54

Note that the cellular connectivity simulated the cutter mock-up and is a representative of next generation satellite communications rather than current on demand satellite service implemented on the patrol boats.

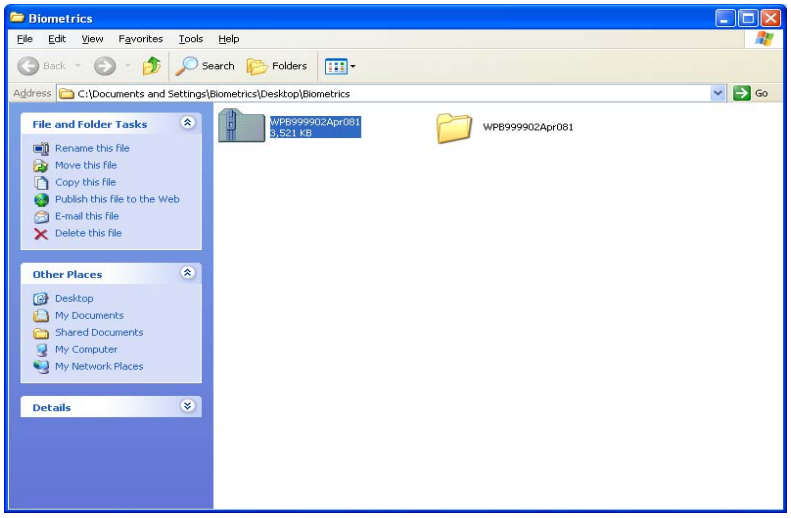
The second test conducted was used to determine the ability of the Command Center mock-up to retrieve the test biometric files from the MLCA server mock-up. The notification email that was received from the MLCA server by the Command Center mock-up contained a link to the test biometric files that were waiting to be downloaded. The image below is a snapshot of the Command Center Mailbox.



Upon clicking the link in the email the user was prompted to save the file to disk. Once the user chose the file name and destination, all files were downloaded from the MLCA server to the Command Center mock-up in less than three seconds.

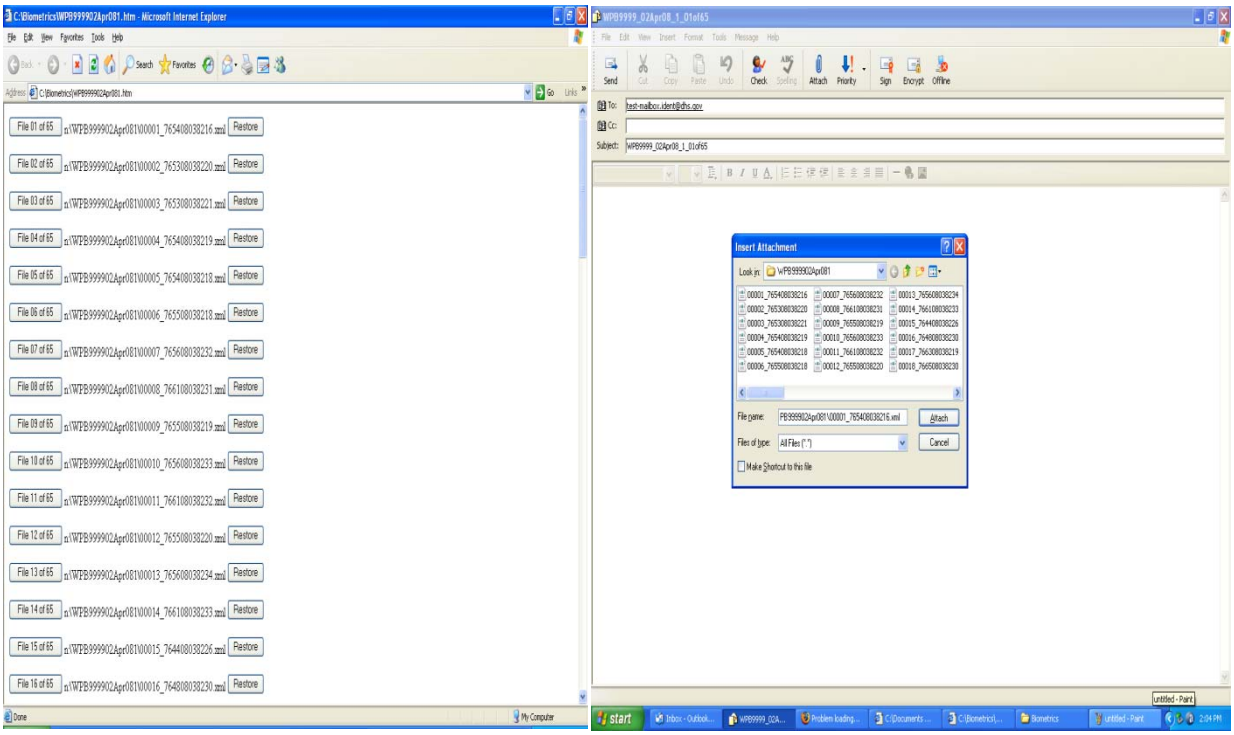


The third test was conducted to analyze how long it would take to send the test biometric files to the US-VISIT database and receive the hit/no hit emails back. The files had to first be unzipped from their zip file.



The biometric files were then attached one at a time to an email and sent individually to the US-VISIT database. Due to limitations set forth by US-VISIT, we were only able to send 10 test emails to US-VISIT. It took 90 seconds for the user to unzip the biometric files and create ten emails with attached test biometric files. The HTML file, which is created by the user interface

on the patrol boat, has every biometric file labeled and the files location. Upon clicking the file an email is automatically generated with the proper email address and subject line. The user attaches the biometric file and the email is ready to be sent.



The emails were sent to the US--VISIT test database and return emails were sent to LTjg Mario Teixeira's (R&D Center sponsor) .mil email address. US-VISIT requires that their return notification emails be sent to a .mil email account. The time at which the emails were sent, as well as, the time the return notification emails were received is contained in the chart below.

Table 2. Test results for transferring data from CC to US VISIT

Email Number	Send time, (local time)	Received, (local time)
1	14:20	14:22
2	14:21	14:23
3	14:21	14:23
4	14:21	14:23
5	14:21	14:23
6	14:21	14:23
7	14:21	14:23
8	14:22	14:23
9	14:22	14:24
10	14:22	14:24

The final test that was conducted combined all three previous tests, and was simply a test of the entire mock-up Biometrics at Sea process. Twelve test biometric files were zipped into a zip file, sent to the MLCA server mock-up, then uploaded to the Command Center mock-up, and sent to US-VISIT. Twelve test files were used because there was a limitation to the amount of files the US VISIT test database wanted to be sent. While each step in this process was individually timed, the main purpose of the test was to get a time of the complete evolution. The following list goes through the time of events through this test.

- 12:32:00 Click to zip 12 test biometric files into zip file
- 12:32:04 Zip complete
- 12:32:20 Open MLCA Large File Transfer web application
- 12:32:30 Browse to select zip file from 110' cutter
- 12:33:10 Uploading files to MLCA server mock-up
- 12:33:15 File upload complete
- 12:33:45 Verification in Command Center mock-up inbox

- 12:35:30 First email sent to US VISIT test database
- 12:36:42 First wrap back email received from US VISIT
- 12:37:20 Last Email sent to US VISIT test database
- 12:39:30 Last wrap back email received from US VISIT

The notification emails that were received from the US VISIT test database were not hit/no hit emails, but, were rather wrap back emails. The wrap back email is simply a notification that the US-VISIT test database has received the file and has processed it through the database. This was because each test biometric file that was sent to the US-VISIT test database was the same "fake" biometric file. Therefore, the US-VISIT test database gets confused when it processes the same "fake" biometric file 12 times. The entire process was completed in 9 minutes and 30 seconds.

Conclusions

In conclusion, as the Coast Guard continues to fight against the everyday threat of illegal immigration, the advancement of the tools and technology used to aid in this mission is critical. The implementation of the original Biometrics at Sea system was a tremendous step in the right direction. However, it has proven to be extremely expensive, time consuming for the cutter, and very inconsistent in its speed of service. By integrating the MLCA Large file transfer system with the current Biometrics at Sea system, an encrypted zip file would be transferred to shore very expeditiously. Once on shore the Command Center would be notified of the files, retrieve them from the MLCA server, send them to US-VISIT individually in an email, and relay all results back to the cutter via radio communications. The cutters would be notified as soon as the transfer of the zip file was complete allowing them to turn off their underway Internet connectivity immediately. They would also be able to focus their attention on the migrant's onboard while the Command Center finishes the process of sending the files to the US VISIT.

By implementing this optimized biometric file transfer system the Coast Guard will decrease satellite air time and increase the availability, reliability, and speed of biometric data transfer.

FUTURE VISION FOR BIOMETRICS

OMBDN senior design project is only an intermediate step towards the vision of the final optimization of the biometric files transfer system design. The desire to move biometrics to the 10 finger print scan will greatly increase size of the files and time of its transmission. Therefore, the need for the server interface at US-VISIT is greater than ever. The realization of this project will move the biometric transfer of data via e-mail function from the dynamic shipboard environment to more static shore side units. This function can be completely automated and moved to US-VISIT to serve all Department of Homeland Security (DHS) agencies. However, the LFT server needs to be practically tested within the USCG organization before moving to the next step of US-VISIT hosting the LFT server. US-VISIT hosting the LFT server combined with the next generation satellite performance will not only radically speed up the transfer process and, subsequently, decrease recurring operating cost but also increase availability and simplicity of the transfer process. Therefore, not only will the USCG have simple, easy and secure access to the US-VISIT database but database interface will also be available to other DHS agencies. The end result will be a truly optimized system design and process serving to enhance the law enforcement capabilities of the operator.

References

[1] Coast Guard Underway Connectivity Policy, "Small Cutter Connectivity Project", available from, http://cgweb.tiscom.uscg.mil/tsd1/tds1b/systems/0009-SCC(v)/00069-SCC(V).htm (accessed 10 Sep 2007).

[2] Teixeira, Mario LTjg. Email Interview. April 20, 2007.

[3] Bailey, Shawn LT. Email Personal Interview. October 15, 2007.

[4] MLCA website, "MLCA Large File Transfer", available from http://webgis.mlca.uscg.mil/uploads, (accessed 10 Sep 2007).

[5] "Technology." Venturi Wireless. 20 Apr. 2008 <http://www.venturiwireless.com/solutions/technology.html>.

[6] COMDT COGARD Washington DC, 301854Z Jan 07. "Underway Connectivity Policy for WPB-110 Class Cutters".

[7] LT S. Bailey. (2007, October 18) "E-Coast Guard Connectivity ORD", email.

[8] Hunley, Don LT. Email Personal Interview. November 30, 2007.

[9] "Allaire ColdFusion." Internet Presence Provider. 2004. 22 Apr. 2008 <http://www.gsp.com/support/virtual/coldfusion/>.

Bibliography

[10] MLCA Website, "MLCA Naval Engineering Homepage", available from, http://www.uscg.mil/mlclant/VDiv/default.htm (accessed 10 Sep 2007).

Appendices

A. Business Case
B. Project Management Plan
C. Functional Requirements Document
D. Design Specification
E. Support Plan
F. Test Plan